WHAT IS CLAIMED IS:

1. A method of detecting an intrusion at a node of a network, comprising:

reading a first packet received by the node;

determining a first signature of the first packet;

comparing the first signature with a signature file comprising a first machine-readable logic representative of a first packet signature;

determining the first signature corresponds with the first machine readable logic;

reading a second packet generated by the node in response to reception of the first packet;

determining a second signature of the second packet;

comparing the second signature with the signature file further comprising a second machine-readable logic representative of second packet signature; and

determining the second signature corresponds with the second machine readable logic.

2. The method according to claim 1, further comprising executing a directive associated with the first machine readable logic upon determining the first signature corresponds with the first machine readable logic.

3. The method according to claim 1, further comprising executing a directive associated with the second machine readable logic upon determining the second signature corresponds with the second machine readable logic.

4. The method according to claim 3, wherein executing a directive associated with the second machine readable logic further comprises discarding the second packet.

5. The method according to claim 4, wherein discarding the second packet further comprises discarding the packet at the network layer of the network stack of the node.

6. The method according to claim 1, wherein reading a second packet generated by the node in response to reception of the first packet further comprises reading a second packet generated by a network stack of an operating system of the node.

7. A computer-readable medium having stored thereon a set of instructions to be executed, the set of instructions, when executed by a processor, cause the processor to perform a computer method of:

reading a first packet;

determining a first signature of the first packet;

comparing the first signature with a first instruction set comprising a first set of machine readable logic representative of a first packet signature;

determining the first signature corresponds with the first set of machine readable logic;

reading a second packet;

determining a second signature of the second packet;

comparing the second signature with a second instruction set comprising a second set of machine readable logic representative of a second packet signature; and

determining the second signature corresponds with the second set of machine readable logic.

8. The computer-readable medium according to claim 7, further comprising an instruction set that, when executed by the processor, causes the processor to perform the computer method of executing, upon determining the first signature corresponds with the first instruction set, a directive comprised of machine-readable instructions, the first instruction set comprising the directive.

9. The computer-readable medium according to claim 7, further comprising an instruction set that, when executed by the processor, causes the processor to perform the computer method of executing, upon determining the second signature corresponds with the second instruction set, a directive comprised of machine-

readable instructions, the second instruction set comprising the directive.

10. The computer-readable medium according to claim 9, wherein executing a directive comprised of machine-readable instructions further comprises executing a directive that causes the processor to discard the second packet.

11. The computer-readable medium according to claim 10, wherein executing a directive that causes the processor to discard the second packet further comprises discarding a packet at a network layer of a network stack.

12. The computer-readable medium according to claim 7, wherein comparing the first signature with a first instruction set comprising a first set of machine readable logic representative of a packet signature further comprises performing a binary pattern comparison with the first signature and the first set of machine readable logic.

13. The computer-readable medium according to claim 7, wherein comparing the second signature with a second instruction set comprising a second set of machine readable logic representative of a packet signature further comprises performing a binary pattern comparison with the second signature and the second set of machine readable logic.

14. A node of a network operable to detect an intrusion thereof, comprising:

a central processing unit;

a memory module for storing data in machine readable format for retrieval and execution by a central processing unit; and

an operating system comprising a network stack comprising a protocol driver, a media access control driver and a network filter service provider bound to the protocol driver and the media access control driver, the network filter service provider operable to receive a first packet and to determine a first signature of the first packet and compare the first signature with a first instruction set comprising a first set of machine readable logic representative of a first packet signature and to determine a correspondence with the first set of machine readable logic, the network filter service provider further operable to receive a second packet and to determine a second signature of the second packet and compare the second signature with a second instruction set comprising a second set of machine readable logic representative of a second packet signature and to determine a correspondence with the second set of machine readable logic, the processor operable to execute a directive comprised of machine readable instructions upon determination, by the network filter service provider, of a correspondence between the first signature and the first instruction set and correspondence between the second signature and the second instruction set.

15. The node according to claim 14, wherein execution of the directive causes the network filter service provider to discard the second packet.

16. The node according to claim 14, wherein the first packet is received by the node and the second packet is generated by the node.

17. The node according to claim 14, wherein the first packet is generated by the node and the second packet is received by the node.

18. The node according to claim 14, wherein the network filter service provider further comprises a pattern matching algorithm, the comparison of the first

signature with the first instruction set and the comparison of the second signature with the second instruction set performed by the pattern matching algorithm.

19. A method of detecting an intrusion at a node of a network, comprising:

reading a packet by the node;

determining a signature of the packet;

comparing the signature with a signature file comprising a machine-readable logic representative of a packet signature; and

determining the signature corresponds with the machine readable logic.

20. The method according to claim 19, wherein the packet is received by the node.

21. The method according to claim 19, wherein the packet is generated by the node and generation of the packet is made in response to reception of a first packet received by the node.

22. The method according to claim 19, wherein the packet is generated by the node, an evaluation made that the packet is a probe packet upon determining the signature corresponds with the machine readable logic.